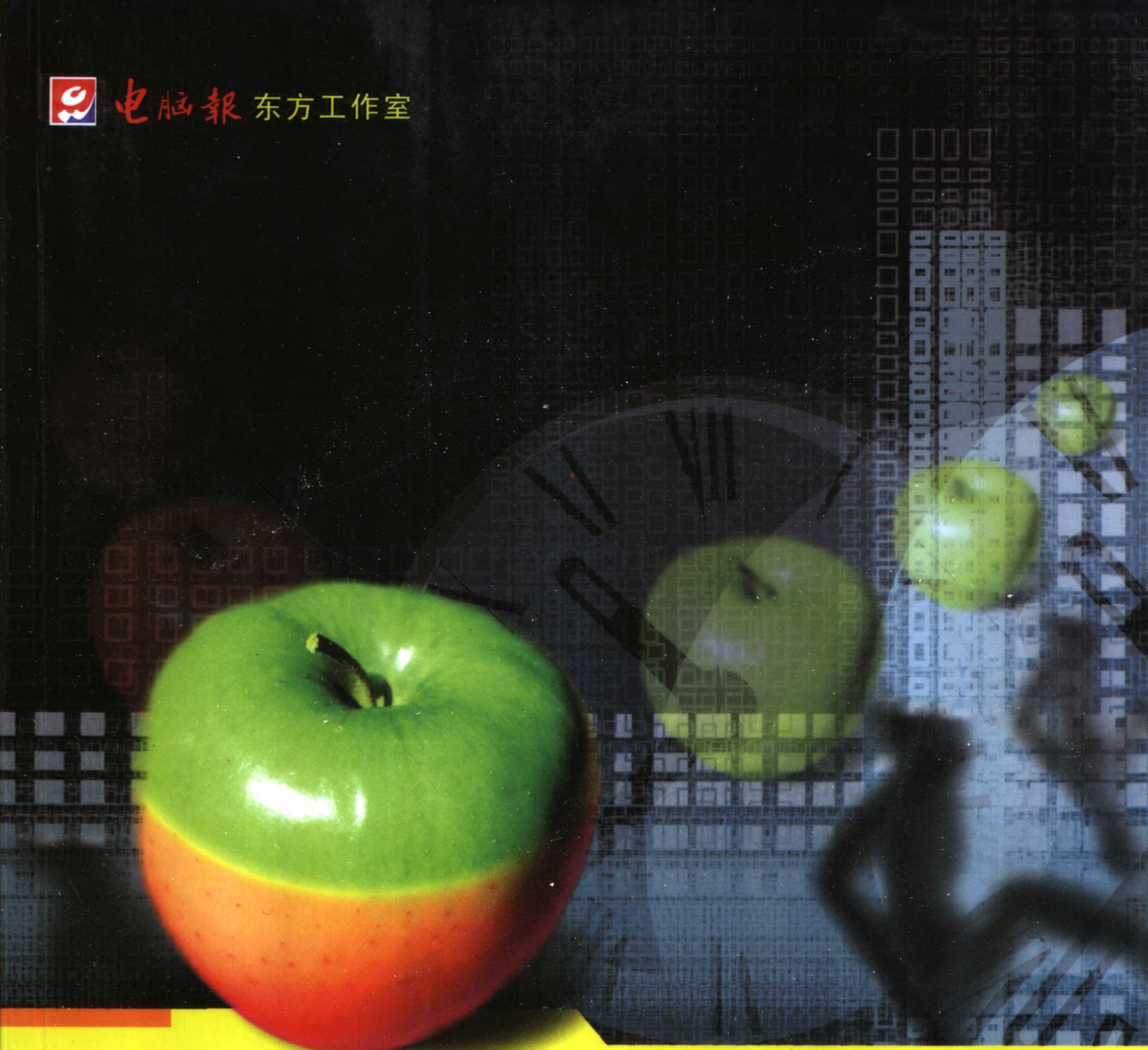
电脑报 东方工作室



系统漏洞大曝光

常见漏洞攻防经典实战手册

编著 瞿英 彭静 刘强

重庆出版社

系统漏洞大曝光

XITONG LOUDONG DABAOGUANG

常见漏洞攻防经典实战手册

编著 翟英 彭静 刘强

重庆出版社

内容提要

本书围绕当前流行的系统平台和应用产品中存在的各种安全漏洞，从一些典型的黑客攻击案例入手讨论相关的防御方法和策略。这些案例涉及应用系统中被黑客和病毒利用最频繁的、危害最大的典型安全漏洞。同时，本书针对黑客利用系统漏洞进行入侵和攻击的方法，以及防御的方法进行了综合的介绍。

本书内容主要面向系统管理员、网络安全工程师等技术人员。同时，也可作为大中专院校计算机专业学生网络安全课程的参考教材或选修课程教材，并可作为网络安全技术爱好者的参考资料。

图书在版编目（CIP）数据

系统漏洞大曝光／瞿英 彭静 刘强编著.—重庆：重庆出版社，2003
ISBN 7-5366-6198-3

Ⅰ.系… Ⅱ.①瞿…②彭…③刘… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2003）第 016977 号

编　　著：瞿 英　彭 静 刘 强
责任编辑：刘爱民　谢 先
封面设计：黄 河
版式设计：杨丽华

系统漏洞大曝光
常见漏洞攻防经典实战手册

重庆出版社出版、发行
新 华 书 店 经 销
重庆升光电力印务有限公司印刷

*

开本：787 × 1092　1/16　印张：17　字数：408 千
2003 年 6 月第 1 版　　2003 年 6 月第 1 次印刷

印数：1～5 000

*

ISBN 7-5366-6198-3/TP · 114
定价 24.00 元
（随书赠送 1CD）

前言

QIAN YAN

随着Internet应用不断渗透到社会生活的各个领域，信息系统的安全开始和越来越多的人的工作和生活紧密联系在一起，越来越多的人开始意识到安全问题已经成为信息时代所要面临的最大的需要刻不容缓解决的首要问题。

网络中层出不穷的黑客事件和泛滥成灾的计算机病毒直接对社会的政治、经济、文化以及军事等各个领域造成了难以估算的巨大损失。而黑客、病毒针对众多的著名电子商务网站的入侵和破坏，则给人们对即将到来的信息时代的美好憧憬蒙上了一层阴影。这将制约信息技术的进一步应用和发展。因此，如何解决信息系统的安全问题已经成为近期，特别是进入2002年以来人们关注的最热门话题。

为什么黑客和计算机病毒可以对我们的系统长驱直入、肆意妄为呢？罪魁祸首就是信息系统的安全漏洞。信息系统的安全漏洞产生的原因很多。我们知道实际上没有也不可能有真正完美的没有缺陷的系统。由于人们的认识总是渐进发展的，因而人们对安全问题认识的局限性总是随着应用的不断发展被一点点暴露出来。因此，努力设计出尽可能安全的系统和积极地进行安全防范是实现信息系统安全的关键

由于信息系统在设计、部署、实施和日常的管理和维护中都存在着这样那样的缺陷和疏忽，这都会给黑客以可乘之机。然而，人们对系统中存在的各种安全漏洞往往毫不知觉或置若罔闻。这是应用系统中最致命的安全问题，所以需要让更多的人了解安全漏洞的危害性并提供完善的解决方案。本书正是应这样的需求而编写。

本书共10章，分别针对信息系统安全的基础知识，常见的黑客攻击及其危害，黑客和计算机病毒进行入侵和破坏所利用的系统漏洞，以及安全漏洞的防范策略和方法等进行了探讨。其中，第1章主要介绍了系统安全及有关黑客的一些常识，第2章介绍了黑客在进行入侵和攻击之

前对目标系统进行探测以发现漏洞所采用的最常用的手段，第3章介绍了黑客利用系统的漏洞直接进行入侵和破坏的典型案例，第4章介绍了针对密码的争夺及其防御策略，第5章介绍了黑客如何利用系统漏洞提升权限，第6章介绍了目前最难防范的拒绝服务攻击，第7章介绍了在操作系统和应用软件中普遍存在的脚本漏洞，第八章介绍了当前对网络用户威胁最大的著名安全漏洞和攻击，第九章介绍了系统漏洞的修补，第10章针对漏洞的攻击介绍了积极防御的方法和策略。

本书不可能对系统中存在的所有安全漏洞进行讨论，因而有选择地选取了一些最典型的案例，根据黑客入侵和攻击的特点分为几个方面，对最频繁被黑客和病毒利用的系统漏洞及攻击行为进行了重点的介绍。笔者在长期从事网络技术服务的过程中，接触了大量的企业用户和普通用户，人们对安全知识的匮乏是令人吃惊的。希望本书的推出能够警示一些用户，改善我们的网络应用环境。

本书内容主要由河北经贸大学信息技术学院翟英（MCSE MCT）编写，其中第1、6、8章的部分内容由彭静编写。此外，大连水产学院的刘强先生编写了书中有关Shadow Security Scaner和微软基线安全分析器的内容，并提供了许多参考资料，在此表示感谢。本书由刘晓辉（MCSE CCNA）审稿。由于笔者技术的局限性，本书内容难免会存在一些纰漏和缺陷，请读者原谅，并真诚欢迎批评指正。

翟英

2003年5月

试读结束，需要全本请在线购买： www.ertongbook.com

目录

CONTENTS

XITONG LOUDONG DABAOGUAN

第1章

系统漏洞与网络安全

随着计算机技术和通信技术的不断发展，现代社会正在逐步迈入信息时代，信息技术的应用不断渗透到人们生活的各个领域。网络应用特别是Internet应用的飞速发展，已经使越来越多的人开始享受到数字时代的崭新的网络生活方式。然而，随着越来越多的安全问题被不断地暴露出来，信息系统的安全开始受到来自各个方面的越来越多的威胁，这给信息技术的进一步发展蒙上了一层阴影，特别是使基于Internet的电子商务的发展受到一定程度的制约。

那么造成安全问题的“罪魁祸首”是谁呢？那就是存在于信息系统中的各种各样的系统漏洞。

1.1 系统漏洞的类型

从各个厂商和安全技术研究机构（如 CERT 等）的安全公告中可以了解到，系统漏洞在所有的系统中是广泛存在的，数量巨大，而且每天都在不断地增加。不仅是原来没有安全防范的系统不能提供安全保障，即便是后来开发的所谓安全计算机产品，甚至是安全防范产品（如防火墙等）在不同环节上也存在不少安全问题。

根据系统漏洞产生的原因，系统漏洞通常可以分为以下几种类型：

（1）软件的 Bug

服务器守护程序、应用程序、操作系统以及协议栈等软件的 Bug 是入侵者经常利用的对象，主要反映在程序编制过程中没有考虑到对特殊输入的处理。这些程序引起的系统的脆弱性包括：

● 缓冲区溢出

缓冲区溢出是拒绝服务攻击中最可能出现的一种。例如，程序员一般不会想到用户账号会有几百个字节，如果一旦有人这样做了，就会导致难以估计的错误。通过仔细研究源代码，就可以利用缓冲区溢出后的系统处理得到超级用户权限。

● 特殊字符组合

这类问题主要出现在 CGI 程序中。例如，用户键入“| mail < /etc/passwd”这样一条命令，系统就会截取管道符“|”并调用“Mail”程序将 Passwd 文件发到用户信箱中。典型的还有 Web 系统中常见的 Unicode 漏洞等。

● 竞争条件

由于操作系统的多任务性，当两个程序同时访问同一段数据时就可能产生错误。

（2）系统配置不当

● 缺省配置

操作系统的默认配置往往照顾用户的友好性，但容易使用的同时也意味着容易受到攻击。

● 系统管理员失职

由于操作系统的复杂性，没有经过严格培训的系统管理员很难做到万无一失。

● 系统后门

为了调试或使用程序方便，往往会留有一些默认口令或非正常进入系统的方法。这些后门一旦被发现，便成为严重的安全漏洞。

● 信任关系

相互有信任委托关系的主机很容易遭到攻击。

（3）脆弱性口令

大部分人的口令由自己或家人的名字组成，或加上简单的数字或与账号相同。攻击者可以通过猜测口令或在拿到文件后，利用密码破解程序和密码字典进行攻击。

（4）信息泄漏

入侵者常用的方法之一就是窃听。在广播式的局域网上，将网卡设置成混杂模式，就可以监听到网络上的所有数据包。如果在服务器上安装窃听软件（Sniffer），就可能拿到远程用户的账号和口令。

（5）设计缺陷

协议缺陷

最典型的就是 TCP/IP 协议，在设计协议时并没有考虑安全因素。虽然现在已经充分意识到这一点，但由

于 TCP/IP 已经广泛使用，因此无法被完全替代。例如 ICMP、IP Spoofing、SYN Floods 等攻击就是利用了协议的缺陷。

操作系统缺陷

虽然操作系统在设计时考虑了很多安全因素，但也不可避免地存在一些缺陷。例如，Windows 的用户权限在启动时由系统注册表获得，这样便会产生许多安全漏洞。

1.2 系统漏洞与网络安全

系统漏洞是危害网络安全的最主要因素，特别是软件系统的各种漏洞。黑客的攻击行为都是利用系统的安全漏洞来进行的。

许多系统都有这样那样的安全漏洞（Bugs），其中有些是操作系统或应用软件由于设计缺陷本身所具有的，这些漏洞在补丁未被开发出来之前一般很难防御黑客的破坏，除非你不接入网络。还有就是程序员在设计一些功能复杂的程序时，预留的用于测试和维护的程序入口，由于疏忽或者其他原因（如将它留在程序中，便于日后访问、测试或维护）没有去掉，这就可能被一些黑客发现并利用作为后门。到目前为止，还没有出现真正安全无漏洞的产品，这也是当前黑客肆虐的主要原因。

黑客利用安全漏洞进行的入侵和破坏所造成的危害主要体现在以下几个方面：

1．系统劫持

在一般情况下，攻击者为了攻击一台主机，往往需要一个中间站点，以免暴露自己的真实所在和身份。即使被发现了，也只能找到中间站点的地址，与己无关。在另一些情况下，假使有一个站点能够访问另一个严格受控的站点或者网络，例如，能够连通到另一个主干网上去，攻击者为了访问另一个主干网的一些站点，往往需要先攻击这个中间站点。

这种情况对目标主机本身并无多大坏处，但是潜在的危机已经存在。首先，它占用了处理器时间，当运行一个网络监听软件时，会占用大量的处理器时间，将使主机的响应时间延长。另一个可能的危害是，这种行为将责任转嫁到目标主机的管理员身上，后果是难以估计的。再就是，可能将一笔账单转嫁给受害者一方。

2．获取文件和传输中的数据

攻击者的目标一般是系统中的重要数据。攻击者可以通过登录目标主机或者使用网络监听程序进行监听等方式来获得。登录或连接到目标主机是最直接的方法，可获得较多的权限，可以直接读取或复制数据文件。此外，监听到的信息可能含有非常重要的信息，如用户密码等。传输中的密码是一个非常重要的数据，当攻击者得到密码，便可以顺利地登录别的主机，或者访问受限的资源。

3．获得超级用户权限

具有超级用户权限，可以做任何事情，所以每一个入侵者都希望能得到超级用户权限。取得这种权限，便可以完全隐藏自己的行踪；在系统中埋伏下一个方便的后门；可以修改资源配置，为自己得到更多的好处。

在 UNIX 系统中，运行网络监听程序必须要有这种权限，因此在一个局域网中，只要掌握了一台主机的超级用户权限，可以说就有可能掌握整个子网。

4．对系统的非法访问

有许多系统是不允许其他用户访问的，比如，一个公司、组织的网络。因此必须以一定手段来得到访问权力，如利用身份验证漏洞、缓冲区溢出漏洞等。

有时系统缺乏访问控制机制，在一个有许多 Windows 95 的网络中，常常有许多用户将自己的目录共享出来，如果密码保护失效的话，别人就可以从容地在这些计算机中浏览、寻找自己感兴趣的东西，或者删除、更换文件。

5．进行不许可的操作

有时候，用户被允许访问某些资源，但通常受到许多限制。在一个 UNIX 系统中，没有超级用户权限，许多事情便无法去做，于是有了一个普通的户头，用户总想得到更大一点的权利。在 Wnidows NT 中也一样。

许多用户都有意或无意地去尝试尽量获得超出允许的一些权限，于是寻找管理员在设置中的漏洞，或者去寻找一些工具来突破系统安全防线，例如，特洛伊木马便是很多用户使用的一种手段。

6．拒绝服务

同上述行为相比较，拒绝服务便是一种有目的的破坏行为了。拒绝服务攻击方式很多，如向目标计算机发送大量的无意义的请求，使得它因无法处理所有的请求而崩溃；制造网络风暴，让网络中充斥大量的信包，占据网络的带宽，延缓网络的传输。

7．涂改信息

涂改信息包括对重要文件的修改、更换、删除，是一种很恶劣的攻击行为，不真实或者错误的信息往往会给用户造成很大的损失。

8．窃取信息

入侵的站点往往有许多重要的信息与数据可用，如用户的账户信息、企业客户信息、系统的安全配置等。因此，黑客入侵还有一个主要目的就是窃取信息，通过入侵来获得别人的电子邮件地址、信用卡信息等个人隐私以及竞争对手的商业机密。

攻击者使用一些系统工具往往会被系统记录下来，如果直接发往自己的站点也会暴露自己的身份和地址。于是窃取信息时，往往将这些信息和数据送到一个公开的 FTP 站点，或者用电子邮件寄往一个可以拿到的地方，等以后再从这些地方取走。这样做可以很好地隐藏自己。将这些重要信息发往公开的站点造成了信息的扩散，由于那些公开的站点常常会有许多人访问，其他的用户完全有可能得到这些信息，并再次扩散出去。

除此之外，还有一些黑客利用系统中的安全漏洞设计出危害更大、更难防范的计算机病毒，有些病毒具有传播木马的能力，使黑客能够在更大的范围里利用“肉机”，发动更为可怕的攻击。这种人为加程序的混合攻击危害更大，常常具有以下特点：

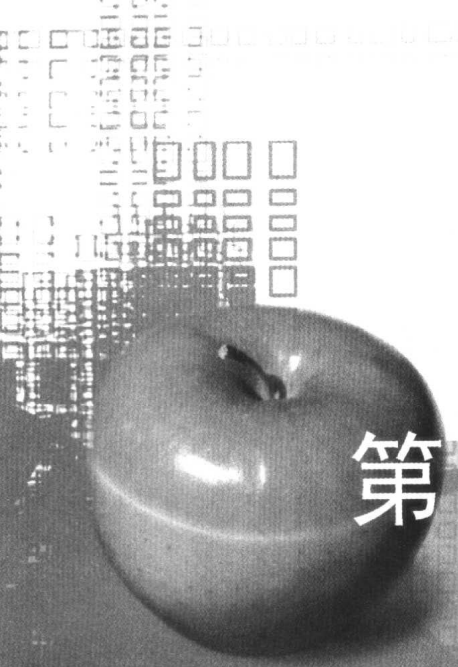
- 整合了病毒和黑客的攻击技术；
- 不需要借助社会工程进行传播和攻击；
- 能够自动发现并自动感染和攻击，如 CodeRed II 和 Nimda；
- 传播速度极快，有可能在几十分钟之内感染整个网络；
- 不需要人工干预，利用软件漏洞进行自动攻击；
- 攻击程序的破坏性更强。

在互联网时代，这一系列的系统入侵和破坏行为的危害就更为严重了。尤其是 Web 系统的安全出现漏洞时，黑客的危害范围就更广泛了。

由于客户系统和服务供应商的系统通过 Internet 已经互联为了一个庞大的、覆盖全球的、错综复杂的整体，信息的安全更难以保障，这也造成了黑客在全球范围内的肆意横行，入侵和攻击可能来自世界任何一个角落。

因此，信息系统安全的研究是目前的当务之急，特别是我国，由于大量的信息技术产品依赖国外企业，并且企事业、机关等的技术人员普遍应用能力低、安全意识差，使我们在这个新的问题面前显得尤其脆弱。历次黑客大战中，受害程度最大的总是我们。

试读结束：需要全本请在线购买： www.ertongbook.com



第2章

旁敲侧击——漏洞的侦测

“柿子拣软的捏”，黑客入侵的目标也总是选漏洞百出的系统。对于大多数的黑客来说，攻击常常是漫无目的的，即使有确定的目标，在正式攻击之前也首先会随机地寻找一个“肉鸡”以便隐藏自己。所以，任何在网络上的计算机都有可能成为被攻击的对象。那么，黑客是如何找到有漏洞的系统的呢？

2.1 隐身

黑客，从人们给他的名称上就可以看出其行为是见不得光的。因此，黑客在进行任何操作之前都必须考虑如何隐藏自身。否则，就很容易被抓住尾巴，那时等待他的恐怕就是牢狱之灾了。

通常在与目标系统直接进行任何通信时，都不可避免地会把自己的 IP 地址暴露给对方。例如，在使用 QQ、ICQ、E-mail 和登录 BBS 等时，IP 地址会直接或间接地被暴露出来。

对于实时连接的通信程序来说，IP 地址很容易被发现。如图 2.1 所示，用 netstat 命令可以实时查看每一个网络连接双方的 IP 地址和服务端口。

用户在登录一些 BBS 系统时，BBS 系统会把其 IP 地址显示在屏幕上（图 2.2）。

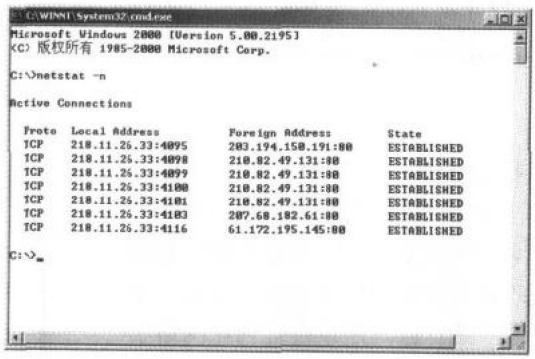


图 2.1 用 netstat 命令查看网络连接

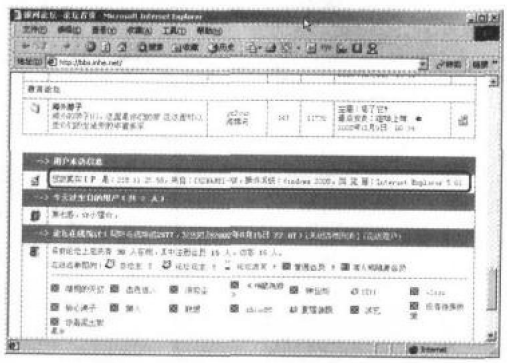


图 2.2 BBS 系统显示的用户 IP 地址

目前流行的即时消息系统常常也会将用户的 IP 地址出卖，用户在使用 QQ 时，IP 地址常常被暴露，极易成为被攻击的目标。

除此之外，邮件系统也会把你的 IP 地址暴露出来，如图 2.3 所示，在 Outlook 中右键选定邮件“选项”，然后，在 Internet 标题中就可以发现发送者和邮件服务器的 IP 地址（图 2.4）。

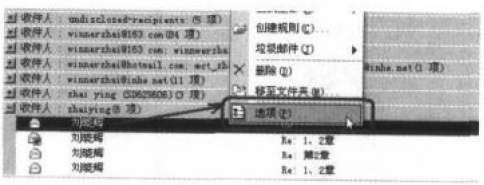


图 2.3 在 Outlook 中选定要查看的邮件

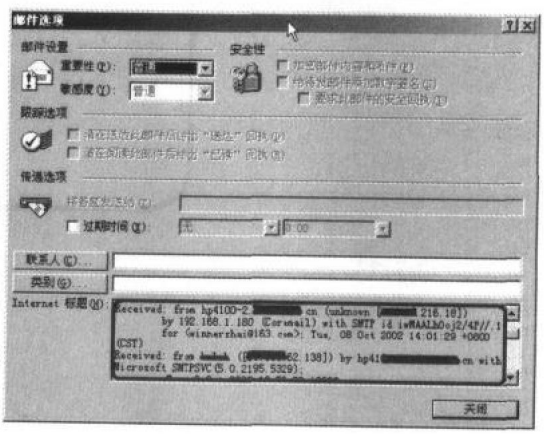


图 2.4 邮件标题中的 IP 地址信息

IP 地址这么容易就被曝光，那么做任何坏事就很难遁形了。为什么会这样呢？

这是由于 Internet 通信程序基于 Socket，Socket 由端口和 IP 地址组成。因此，在建立网络连接时不可避免地会将 IP 地址出示给对方，否则是无法建立程序连接的。

显然，要想隐藏自己的真实 IP 地址就不能与对方直接建立连接。通常，隐藏的方法有以下几种：

1. 通过 Proxy（代理）

通过 Proxy 服务器匿名连接目标主机，是最常用的方法。这种方法也适用于普通用户在访问 Internet 时隐匿自己的 IP 地址。

使用 Proxy 服务器方法有两种：

一种为在线 Web 代理，如 www.pureprivacy.com

等站点，用户可以在其 Web 站点上直接输入要访问的目标主机的 URL 路径，如图 2.5 所示，输入 http://www.yahoo.com，即可间接地访问 Yahoo（图 2.6）。不过，这种方法显然不适合黑客。

图 2.5　在线 Web 代理

图 2.6　通过代理访问 Yahoo

黑客更多地采用另一种方法，即通过配置 Internet 连接使用 Proxy 服务器。首先，黑客必须选择好用的匿名 Proxy 服务器。寻找匿名 Proxy 服务器的方法有很多，有许多站点和软件专门提供这类信息，如图 2.7 所示，www.multiproxy.org 就维护着一个可用匿名 Proxy 服务器的列表。

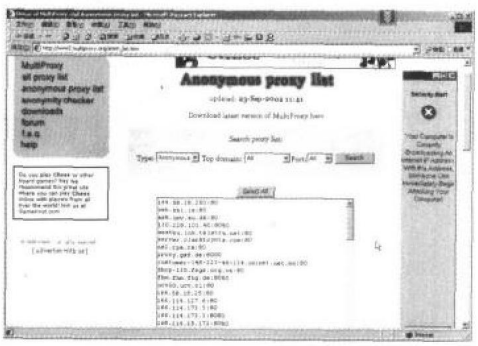


图 2.7　匿名代理服务器列表

选择好匿名 Proxy 服务器以后，下一步就是配置自己的 Internet 连接使用匿名 Proxy。设置的方法如下：

第 1 步　在“控制面板”中选择“Internet”，也可在 IE 的“工具”菜单中选择“Internet 选项”或者右键选择 IE 的“属性”，在“Internet 属性”设置页面点击“连接”（图 2.8）。

第 2 步　根据物理网络连接的情况，选择拨号连接或局域网连接的设置按钮，清除“自动检测设置”，然后设置要使用的代理服务器的 IP 地址和端口（图 2.9）。

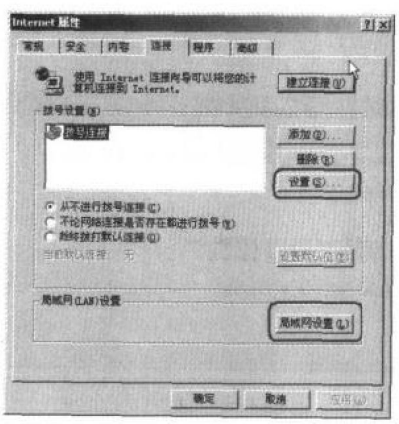


图 2.8　设置 Internet 连接

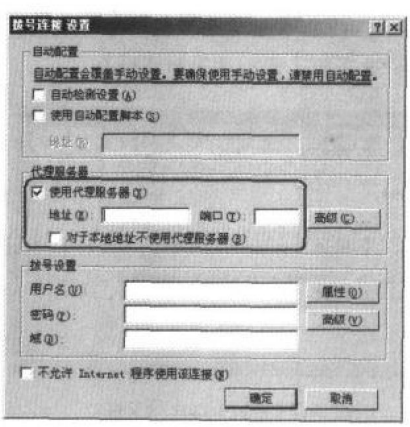


图 2.9　设置 Internet 连接使用代理服务器

第 3 步　点击代理服务器的“高级”按钮，可进一步设置使用 HTTP 等协议时所使用的代理服务器及其端口（图 2.10）。

然后，就不必担心自己的 IP 地址被暴露了。

2. 通过“肉鸡”

通过“肉鸡”连接目标系统是黑客最常用的方法，也是最为隐蔽的方法。这种方法需要预先获得某台或多台主机的控制权，在其中植入木马程序或 SOCK 代理程序，然后就可以以这些“肉鸡”为跳板，通过它们间接与目标系统建立连接，从而达到隐身的目的。

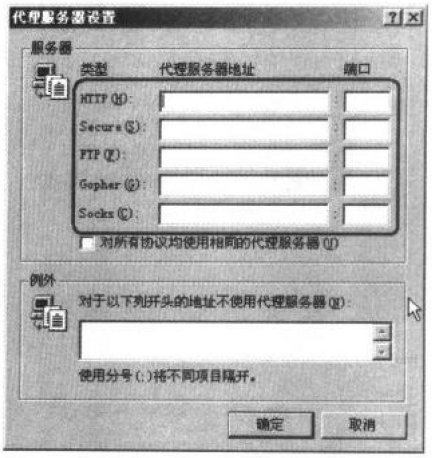


图 2.10 设置 HTTP 等协议所使用的代理服务器及其端口

首先，必须利用已知的安全漏洞控制一台或多台主机，制作“肉鸡”。然后，可以采取两种方法隐藏自己：一是在“肉鸡”上开启 Telnet 或安装 NetCat 等黑客工具，然后就可以直接控制这台“肉鸡”探测和攻击目标系统。另一种方法就是安装 SOCK 代理程序，使之变成 SOCK 代理服务器，成为一个“跳板”，这种“跳板”可以有多个（图 2.11），这样就更不易被追踪。

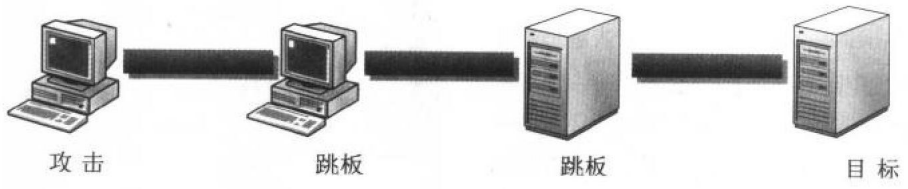


图 2.11 通过“跳板”建立连接

以下看一个使用 SOCK 代理做“跳板”的示例。

第 1 步 选择一个已经被控制的 Windows 主机，建立 IPC$会话连接，然后拷贝 srv.exe、ntlm.exe、sksockserver.exe（SnakeSockServer）到其“肉鸡”上（图 2.12）。srv.exe、ntlm.exe 可在流光中找到。

第 2 步 用 net time 命令查看目标系统的当前时间，再用 AT 命令使 srv.exe 在某个时间启动，然后就可以 Telnet 到其 99 端口上去了（见图 2.13）。

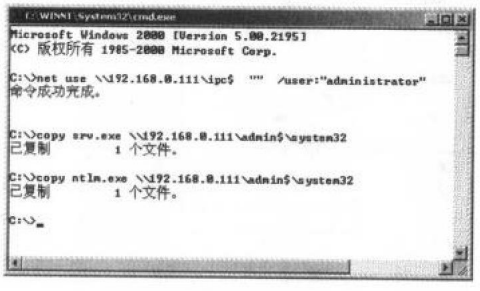


图 2.12 拷贝 srv.exe 等文件

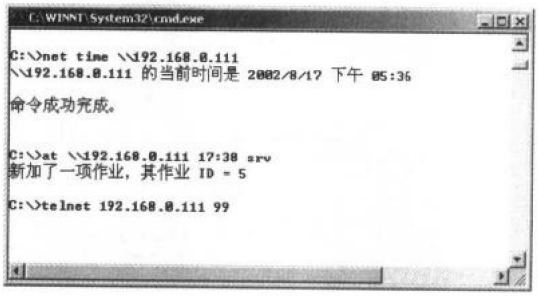


图 2.13 远程用 at 启动 srv

第 3 步 由于 srv.exe 只能连接一次，为了长期入侵，运行 ntlm.exe，然后启动 Telnet 服务（图 2.14）。

第 4 步 运行 SOCK 代理程序 SnakeSockServer 安装程序。执行以下命令：

```
C:>SkSksockServer.exe –install
```

第 5 步 用 SkSksockServer.exe –config 配置 SOCK 服务器。SkSksockServer.exe 的命令参数如图 2.15 所示。

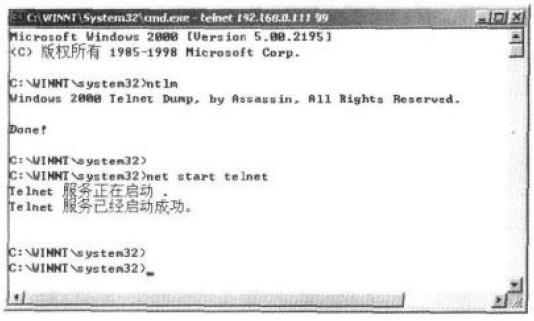


图 2.14　启动 Telnet 服务

图 2.15　SkSksockServer.exe 命令参数

第 6 步　设置好 SOCK 代理服务器，用 net start skserver 启动 SkServer。

第 7 步　如果可以用 Windows 终端连接上去，则可以用图形界面工具 SockServerCfg.exe 进行设置，如图 2.16 所示，如果有足够权限可安装为一个服务。

第 8 步　设置 SOCK 代理连接的客户端，限制连接者（图 2.17）。

图 2.16　设置服务参数

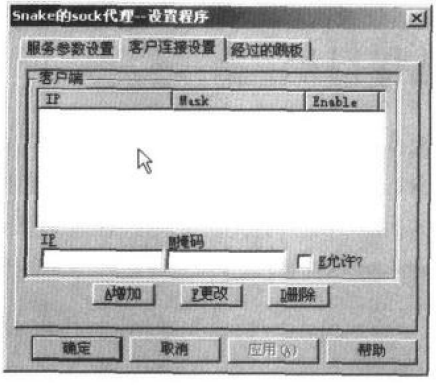


图 2.17　设置 SOCK 代理连接的客户端

当使用多级跳板时，需要做如图 2.18 所示的设置。

除此之外，Snake 还有一个图形界面的服务端程序（图 2.19）。

图 2.18　设置跳板

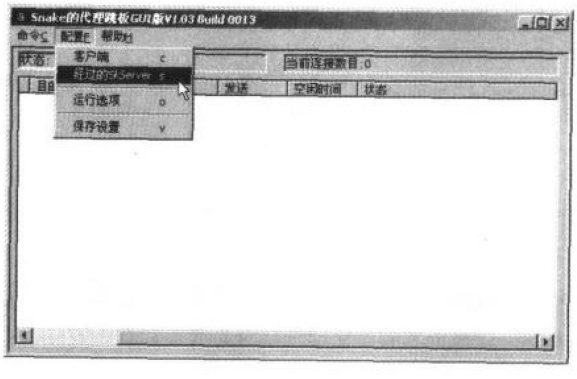


图 2.19　Snake 图形界面的服务端

第 9 步　有了代理，就可以用 SOCK 代理的客户端程序进行连接了。下载并安装 SocksCapV2，运行前首先需进行设置（图 2.20）。

第 10 步　将要运行的程序图标拖入 SocksCap 窗口，点击“Run”运行即可（图 2.21）。

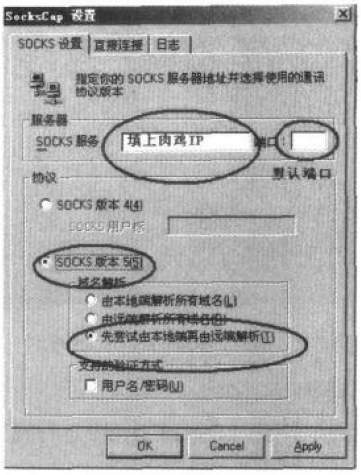


图 2.20 SocksCap 设置

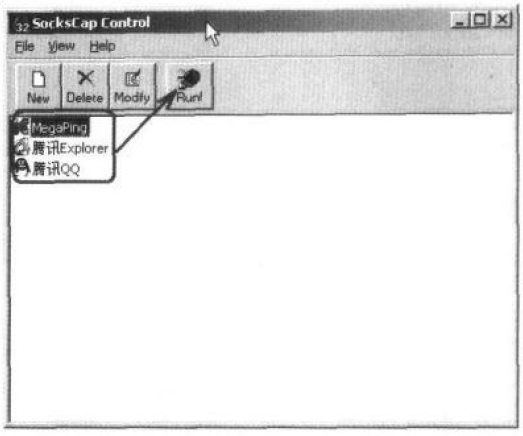


图 2.21 拖入并运行程序

2.2 选择目标

黑客在选择攻击目标或“肉鸡”时，通常是通过 IP 扫描工具进行选择。选择的理由主要有两个方面：一是潜在攻击目标处于特定网络地址范围，如国内黑客针对日本和台湾等地区的攻击；二是黑客为隐藏自身，通常会选择其他地域的“肉鸡”，如国内黑客在攻击台湾网络时，可能会选择日本或韩国的“肉鸡”。

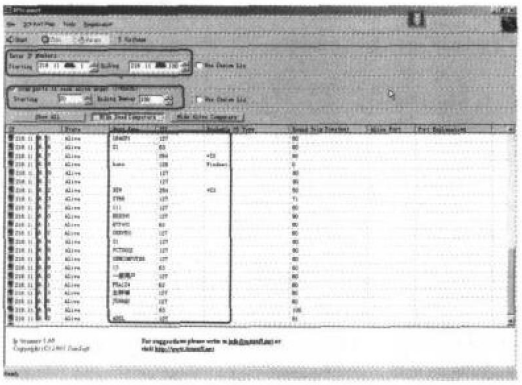


图 2.22 IPScanner

那么，黑客是如何确定攻击目标的呢？

首先，目标系统应该是一台活跃的主机；其次，该主机存在明显的安全漏洞，易于入侵和攻击。

搜寻活跃主机的方法很多，Ping 扫描是最简单的办法，不过手工进行就太笨了，定制一个 Ping 工具或者扫描脚本是很容易的。通常，黑客大多使用专用的 IP 扫描工具，如 IPScanner。

运行 IPScanner，指定扫描的地址范围和端口范围，然后开始扫描，如图 2.22 所示，当前活跃的主机被搜索出来，并且得到了主机名和操作系统类型。

使用 IPScanner 在选择目标时，很难确定目标系统入侵的难易程度。黑客更多的是使用一些对系统漏洞具有较强针对性的扫描工具，如 SuperScan 能够对特定的端口如 23、99、3389 等进行扫描，这样可以直接找到弱点主机。

如图 2.23 所示，用 SuperScan 扫描开放 3389 端口的主机。

那么，如何防止黑客发现你的主机呢？主要有两种手段：

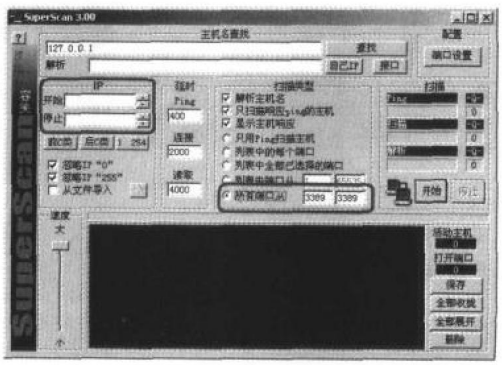


图 2.23 SuperScan

试读结束：需要全本请在线购买：www.ertongbook.com